Aon
Empower Results®

2019 Cyber Security Risk Report:

What's Now and What's Next

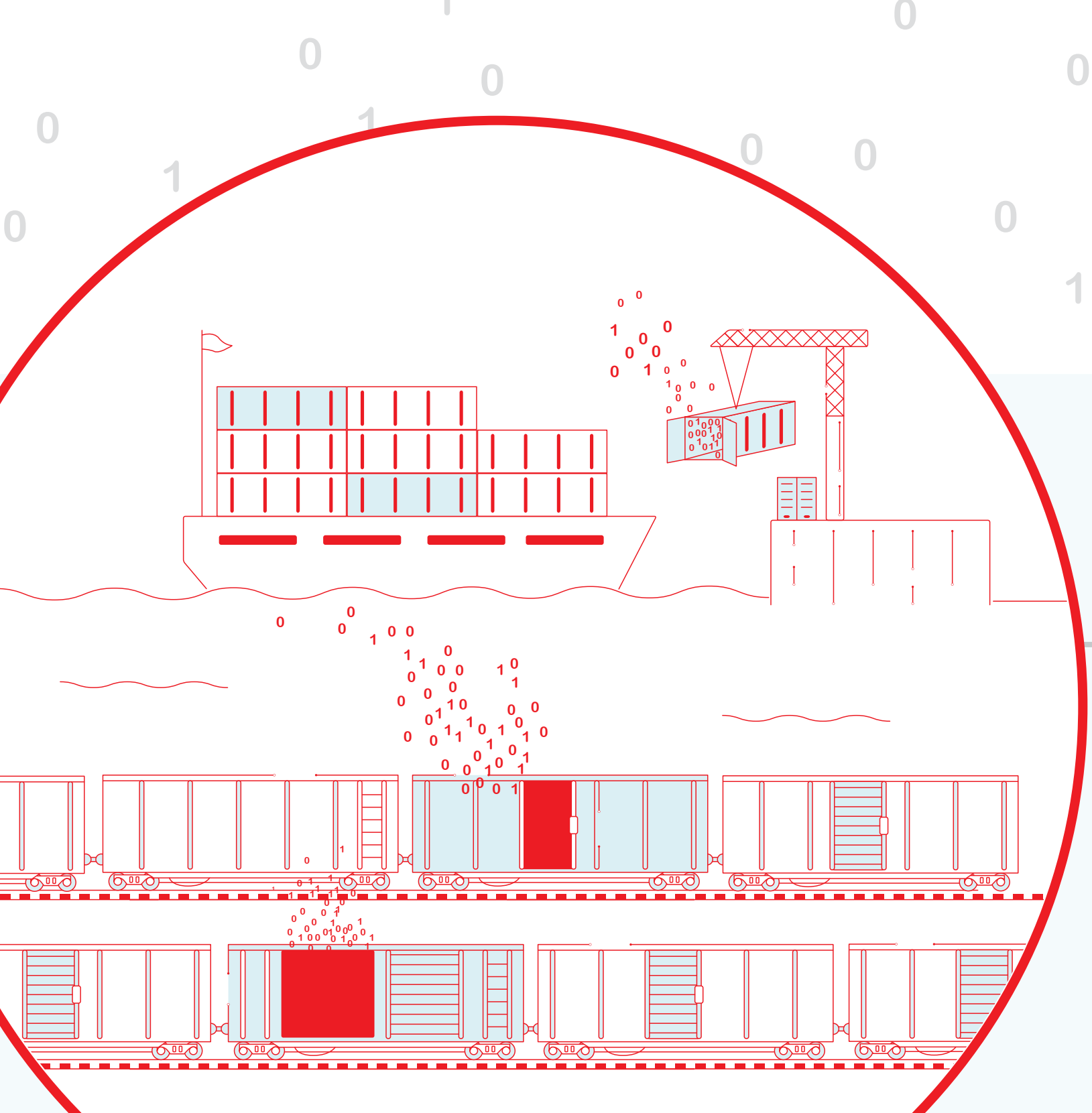
Risk 1
Technology

Embracing digital transformation creates new and unanticipated risks

As traditional "brick-and-mortar" companies rapidly evolve into digital economy XaaS providers, they face new and potentially not-yet-recognized exposures.

XaaS

Organizations must carefully consider new digital risks as digital transformation drives them to new ways of doing business.



Risk 2
Supply Chain Security

Supply chain security wake-up calls grow more insistent

New security issues arise from "direct-to-cloud" employee access and aggregation of data from multiple corporations into shared platforms.

59%

of companies in the U.K. and U.S. said they experienced a data breach via a third party.

2018 Ponemon Study on Global Megatrends in Cybersecurity; https://www.ponemon.org/blog/ponemon-institute-announces-the-release-of-the-2018-megatrends-study

Risk 3
IoT
(Internet of Things)

IoT is everywhere, and it is creating more risks than companies realize

Network-connected IoT devices such as conferencing systems, security cameras, printers, and building automation sensors and controls can easily outnumber the organization's managed IT assets; yet most companies don't securely manage or even inventory all of their IoT devices.

52%

of organizations that maintained an IoT inventory said they had at least 1,000 IoT devices—while the actual study average was much higher, at more than 15,000.

2018 Ponemon Study on Global Megatrends in Cybersecurity; Second Annual Study on The Internet of Things (IoT): A New Era of Third-Party Risk, Ponemon Institute

Risk 4
Business Operations

Technology for operational efficiencies can lead to security deficiencies that disrupt organizations

Increasingly, companies rely on technology to run critical day-to-day business operations. This reliance inherently creates a painfully disproportionate risk of operational disruption. If unprotected, malware infections can shut down manufacturing systems or potentially even a power grid. Ransomware intrusions may bring business operations to a halt by encrypting a company's data.

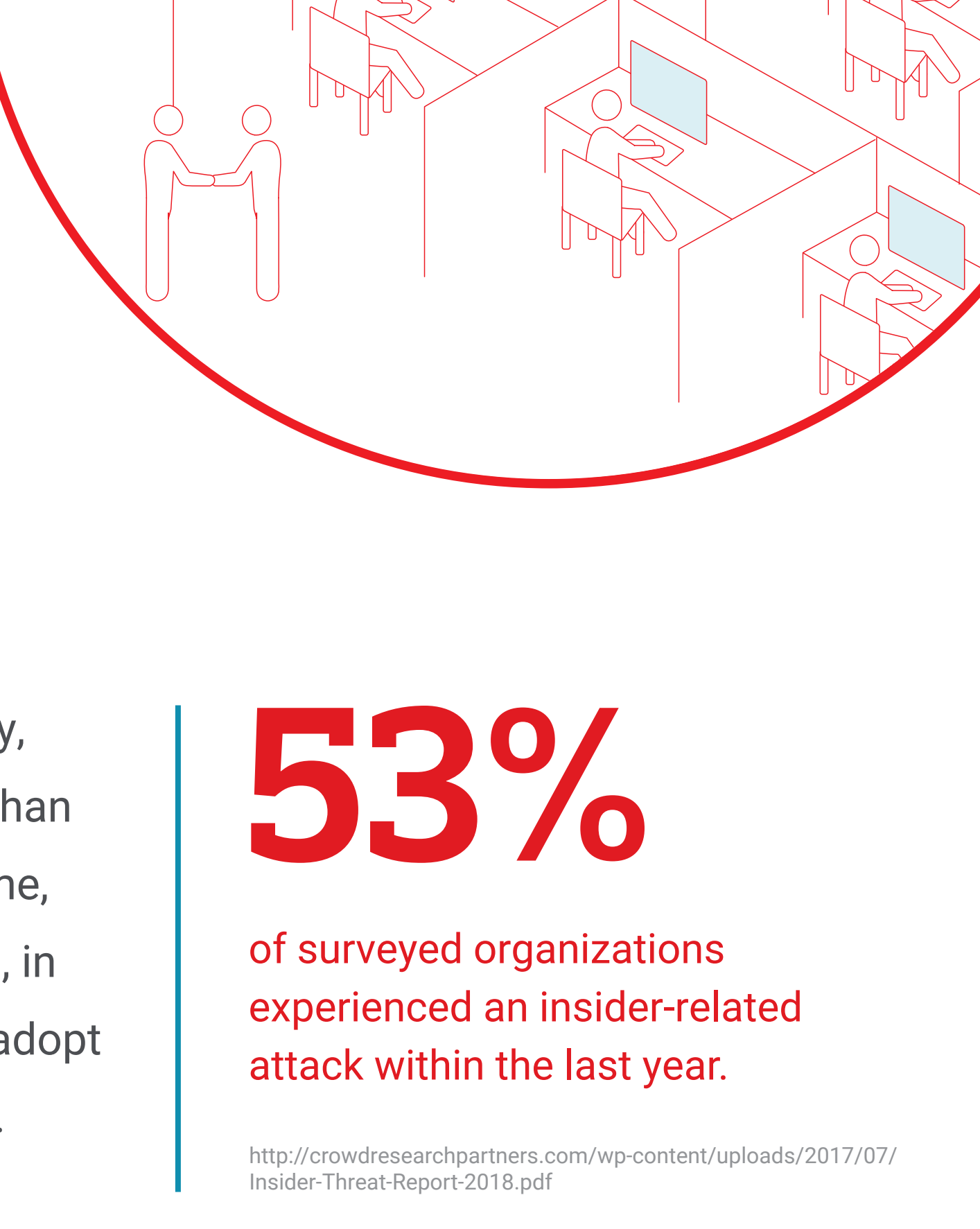
WannaCry ransomware attacked more than

230,000

computers and caused worldwide chaos.

https://www.zdnet.com/article/wannacry-ransomware-crisis-one-year-on-are-we-ready-for-the-next-global-cyber-attack/

Risk 5
Employees



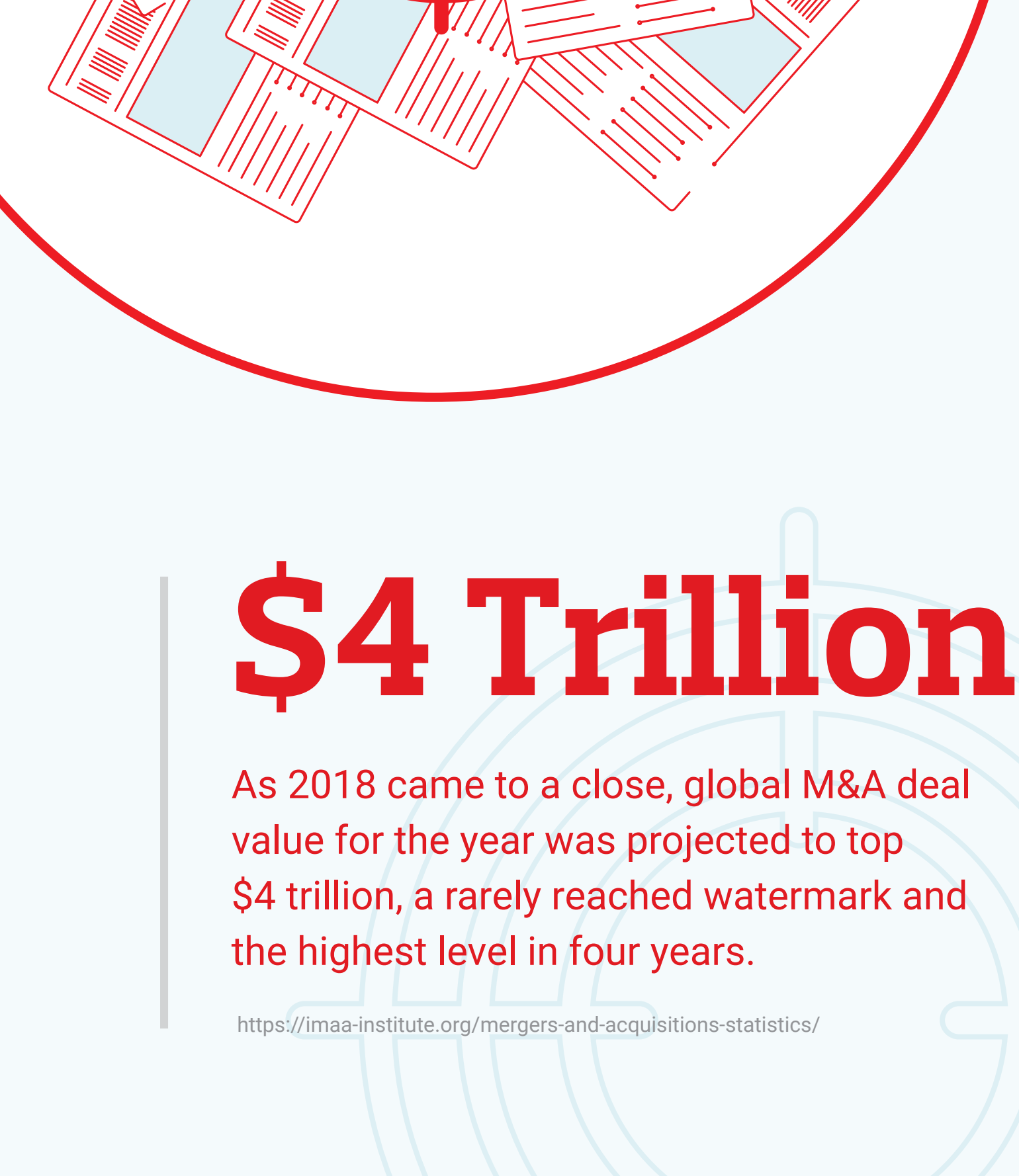
Excess privileges and shadow IT increase employee risk

As companies increase efficiency through technology, they often give users more robust access privileges than may be needed, which increases risk. At the same time, cloud computing intensifies the "shadow IT" problem, in which departments or business units independently adopt technology without telling the central IT organization.

53%

of surveyed organizations experienced an insider-related attack within the last year.

http://crowdresearchpartners.com/wp-content/uploads/2017/07/Insider-Threat-Report-2018.pdf



Risk 6
Mergers & Acquisitions

Vulnerabilities from deal targets increase as dramatically as M&A value

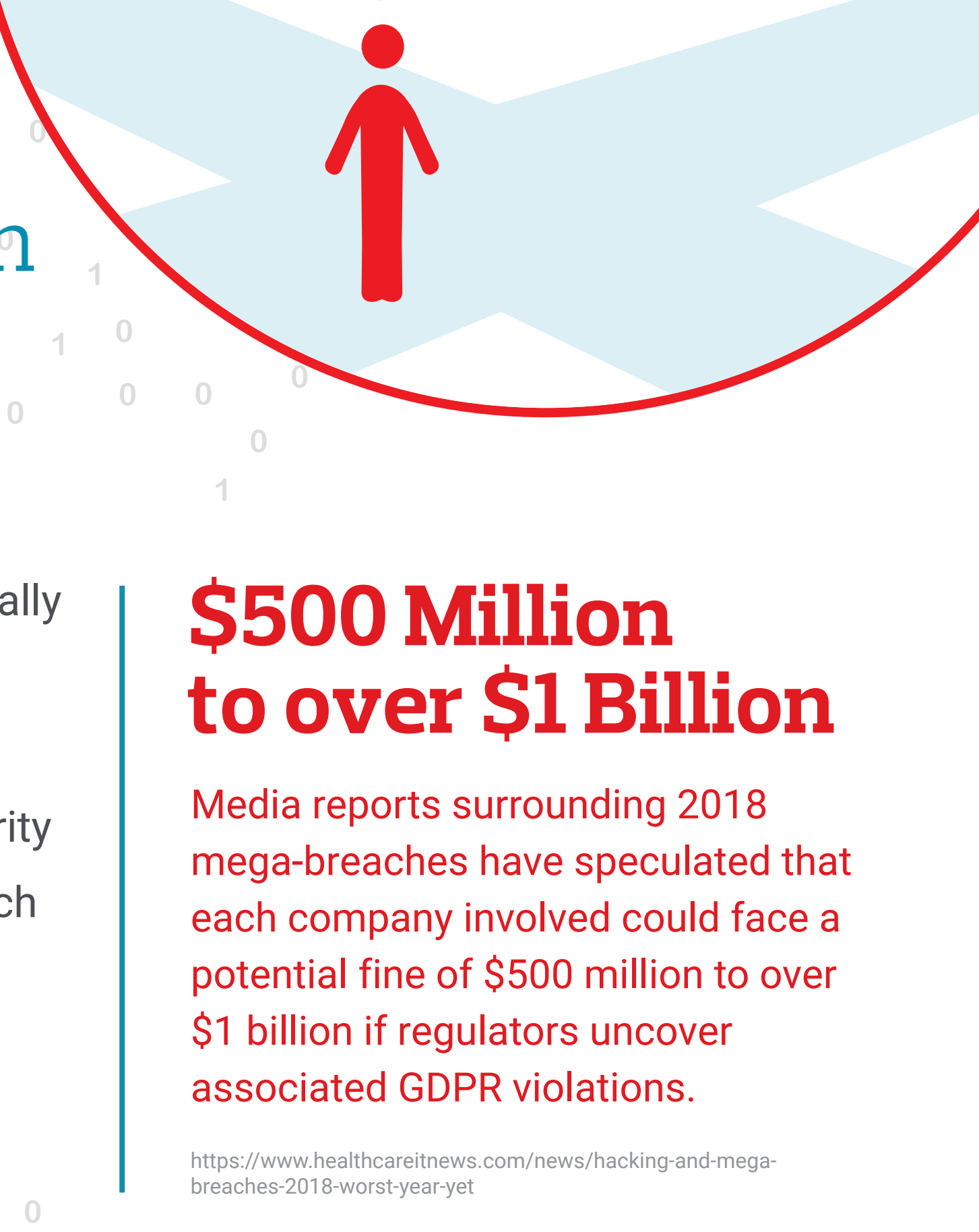
As dealmaking continues to grow, related cyber security risk may rise even faster. Often, bad actors often target companies being acquired by larger enterprises in between deal announcement and closing.

$4 Trillion

As 2018 came to a close, global M&A deal value for the year was projected to top $4 trillion, a rarely reached watermark and the highest level in four years.

https://imaa-institute.org/mergers-and-acquisitions-statistics/

Risk 7
Regulatory



Managing the intersection of cyber security policy and enforcement

Proliferating and overlapping cyber regulations actually tend to create more cyber risk for the CISO. Overwhelming compliance obligations inspire a "check-the-box" mentality replacing best cyber security practices. Even knowing which box to check, in which jurisdiction, has become much more complex.

https://www.rtinsights.com/fresh-data-bdo-sees-some-boards-preparing-for-cyber-risks-others-blind/

$500 Million to over $1 Billion

Media reports surrounding 2018 mega-breaches have speculated that each company involved could face a potential fine of $500 million to over $1 billion if regulators uncover associated GDPR violations.

https://www.healthcareitnews.com/news/hacking-and-mega-breaches-2018-worst-year-yet

Risk 8
Board of Directors

Directors and officers face growing personal liability relative to cyber security oversight

Managing cyber security risk has quickly become one of the biggest oversight challenges facing board directors and officers—and it's a growing personal risk, too. Shareholders have been bringing claims against directors in some of the highest-profile data breaches.

https://www.americanbar.org/content/dam/aba/administrative/litigation/materials/2018-insurance/written-materials/cyber-attack.pdf

3/4

The good news is that nearly three-quarters of board directors say they are more involved with cyber security than they were a year ago.

Download the report

Aon
Empower Results®

Cyber security services offered by Stroz Friedberg Inc. and its affiliates. | © Aon plc 2019. All rights reserved.